Dépannage de l'échec d'authentification basée sur certificat du point d'accès via FTD

Table des matières

Problème

Ces symptômes sont signalés après la migration du Cisco Adaptive Security Appliance 5508 vers Cisco Secure Firewall (CSF) Threat Defense (FTD) 1230 dans la succursale principale (HQ) :

1. Les points d'accès situés dans les filiales ne parviennent pas à s'authentifier auprès du serveur RADIUS au siège social à l'aide de l'authentification par certificat.

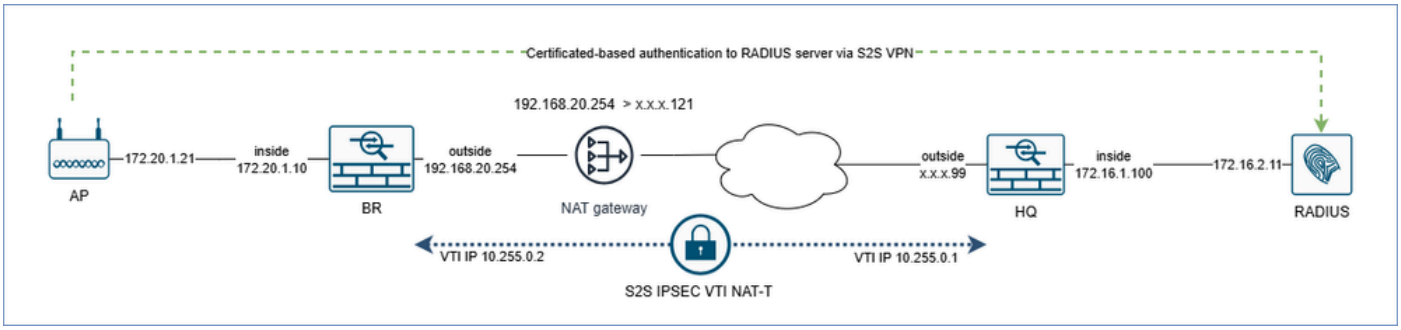
2. L'authentification avec le nom d'utilisateur et le mot de passe a réussi.

Les symptômes sont observés pour les points d'accès dans toutes les branches.

Environnement

CSF 1230 géré par FMC en configuration haute disponibilité exécutant la version 7.7.10.1 au siège social et plusieurs Firepower 1010 autonomes exécutant la version 7.4.2.4 dans les filiales, d'autres versions logicielles peuvent également être affectées. Les symptômes dans ce cas sont indépendants du matériel.

Topologie



image_en_ligne_0.png

Points clés de la topologie :

- Au niveau de la couche réseau, le point d'accès se trouve dans le sous-réseau du pare-feu BR (filiale) à l'intérieur de l'interface.
- Le routeur en tant que passerelle NAT traduit le pare-feu BR extérieur à l'adresse IP de l'interface en une adresse publique x.x.x.121. Cela signifie que le pare-feu BR est à au moins 1 saut du pare-feu HQ.
- Les pare-feu HQ et BR sont connectés à l'aide de réseaux privés virtuels de site à site (VPN S2S) à l'aide d'IPsec (Internet Protocol Security) avec ESP (Encapsulating Security Payload) et de VTI (Virtual Tunnel Interface) sur NAT.
- Au niveau du réseau, le serveur RADIUS se trouve dans le sous-réseau du pare-feu HQ à l'intérieur de l'interface.

Résolution

Pour l'analyse technique, les captures de paquets ont été collectées à partir des pare-feu HQ et BR.

Sur les interfaces physiques des captures d'entrée/de sortie du plan de données du pare-feu HQ et BR, sur les interfaces VTI, les captures d'abandon ASP pour le trafic interne et externe en fonction de l'adresse IP de l'homologue :

Pare-feu BR :

```
cap br_inside interface inside packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16
cap br_vti interface vti-hq packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16.2.
cap br_asp match ip host x.x.x.99 any
cap br_asp match ip host 172.20.1.21 host 172.16.2.11
cap br_outside interface outside packet-length 9000 buffer 33554400 match ip host x.x.x.99 any
```

Notez que x.x.x.99 est remplacé par une adresse IP réelle.

Pare-feu HQ :

```
cap hq_inside interface inside packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16
cap hq_vti interface vti-br packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16.2.
cap hq_asp match ip host x.x.x.121 any
cap hq_asp match ip host 172.20.1.21 host 172.16.2.11
cap hq_outside interface outside packet-length 9000 buffer 33554400 match ip host x.x.x.121 any
```

Notez que x.x.x.121 est remplacé par une adresse IP réelle.

En outre, sur le pare-feu HQ, collectez les captures de commutateurs internes bidirectionnelles dans les interfaces du châssis en fonction du nom externe if et de toutes les interfaces de liaison ascendante :

```
cap hqfxos switch interface outside direction both packet-length 2048 match ip x.x.177.121
cap hqfxos switch interface in_data_uplink1 direction both packet-length 2048 match ip x.x.x.121
cap hqfxos switch interface in_data_uplink2 direction both packet-length 2048 match ip x.x.x.121
cap hqfxos switch interface in_data_uplink3 direction both packet-length 2048 match ip x.x.x.121
no cap hqfxos switch stop.
```

Analyse technique

Pare-feu HQ

1. Les captures d'abandon ASP (Accelerated Security Path) dans le pare-feu HQ indiquent que les fragments sont abandonnés avec la raison fragment-reassembly-failed :

<#root>

>

show capture hq_asp

```
Target:     OTHER
Hardware:   CSF-1230
Cisco Adaptive Security Appliance Software Version 99.23(37)127
ASLR enabled, text region aaaae5d50000-aaaae902d504
172.20.1.21.38676 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (
```

fragment-reassembly-failed

```
) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
172.20.1.21.38676 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (
```

fragment-reassembly-failed

```
) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
172.20.1.21.56952 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (

fragment-reassembly-failed

) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
```

2. Le compteur Timeout pour l'interface VTI dans le résultat de la commande show fragment dans le pare-feu HQ augmente :

```
<#root>

>

show fragment

Interface: vti-br
    Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Run-time stats: Queue: 0, Full assembly: 0
    Drops: Size overflow: 0,

Timeout: 1217

,
           Chain overflow: 0, Fragment queue threshold exceeded: 0,
           Small fragments: 0, Invalid IP len: 0,
           Reassembly overlap: 0, Fraghead alloc failed: 0,
           SGT mismatch: 0, Block alloc failed: 0,
           Invalid IPV6 header: 0, Passenger flow assembly failed: 0
           Cluster reinsert collision: 0
```

Selon la référence de commande (https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html#wp4144096608), le Timeout est "Le nombre maximal de secondes pour attendre l'arrivée d'un paquet fragmenté entier". La valeur par défaut est de 5 secondes. Cela signifie que si la chaîne de fragments entière n'arrive pas au pare-feu dans les 5 secondes, les fragments reçus sont abandonnés et le réassemblage des fragments échoue.

3. D'après le point précédent, le pare-feu HQ ne reçoit pas la chaîne complète de fragments qui entraîne une défaillance du réassemblage de fragments.

Pare-feu BR

1. En fonction des captures, le point d'accès envoie une demande d'authentification basée sur

un certificat RADIUS dans 2 fragments distincts au pare-feu BR. La capture br_inside affiche 2 fragments d'entrée de 1 514 octets et 475 octets respectivement. Les mêmes paquets sont visibles dans les captures d'interface BR VTI qui montrent le paquet avant le chiffrement :

172.20.1.21	172.16.2.11	IPv4			1514	0xf20b (61963)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20b) [Reassembled in #9]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20b (61963)	64	Access-Request id=255
172.20.1.21	172.16.2.11	IPv4			1514	0xf20c (61964)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20c) [Reassembled in #11]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20c (61964)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20d (61965)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20d) [Reassembled in #13]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20d (61965)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20e (61966)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20e) [Reassembled in #15]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20e (61966)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20f (61967)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20f) [Reassembled in #17]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20f (61967)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf210 (61968)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f210) [Reassembled in #19]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf210 (61968)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf211 (61969)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f211) [Reassembled in #21]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf211 (61969)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf212 (61970)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f212) [Reassembled in #23]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf212 (61970)	64	Access-Request id=255, Duplicate Request

image_en_ligne_0.png

L'unité de transmission maximale (MTU) de l'interface externe BR est de 1 500 octets. Pour cette raison, le fragment de 1 514 octets doit être fragmenté en 2 paquets avant le chiffrement.

2. Les captures d'abandon ASP br_asp pour le trafic RADIUS interne sur le pare-feu BR n'affichent pas les paquets abandonnés. Pendant ce temps, pour le trafic externe, il y a des abandons de paquets de 226 octets avec la raison unknown-packet :

<#root>

```
firepower#

show capture br_asp

Target:     OTHER
Hardware:   FPR-1010
Cisco Adaptive Security Appliance Software Version 9.20(2)121
ASLR enabled, text region 560817d6b000-56081d1ae26d
103 packets captured
   1: 10:13:22.160239       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
   2: 10:13:23.160727       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
   3: 10:13:24.161200       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
```

192.168.20.254	.99	ESP	4500	4500	226	0x7254 (29268)	64	6275	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x7e97 (32407)	64	6278 ✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x0fc6 (4038)	64	6281 ✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x3511 (13585)	64	6284 ✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x5868 (22632)	64	6287 ✓	ESP (SPI=0x1592a843)

image_inline_1.png

Notez que la sortie de la commande show capture br_asp affiche 184 octets de longueur de charge utile, alors que la longueur totale de chaque paquet est de 226 octets.

3. Pour vérifier si les paquets ESP abandonnés de 226 octets sont pertinents pour le trafic

affecté entre AP et le serveur RADIUS, la capture br_inside a été relue dans les travaux pratiques internes en utilisant les mêmes configurations de politique de sécurité à partir des pare-feu HQ et BR. La capture br_vti du périphérique de travaux pratiques affiche des fragments de 1 514 octets et de 475 octets, c'est-à-dire avant le chiffrement :

Source	Destination	Protocol	Sport	Dport	Length	IP ID	IP TTL	Info
172.20.1.21	172.16.2.11	IPv4			1514	0xe69d (59037)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69d) [Reassembled in #9
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69d (59037)	63	Access-Request id=218
172.20.1.21	172.16.2.11	IPv4			1514	0xe69e (59038)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69e) [Reassembled in #11
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69e (59038)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe69f (59039)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69f) [Reassembled in #13
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69f (59039)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a0 (59040)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a0) [Reassembled in #15
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a0 (59040)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a1 (59041)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a1) [Reassembled in #17
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a1 (59041)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a2 (59042)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a2) [Reassembled in #19
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a2 (59042)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a3 (59043)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a3) [Reassembled in #21
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a3 (59043)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a4 (59044)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a4) [Reassembled in #23
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a4 (59044)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a5 (59045)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a5) [Reassembled in #25
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a5 (59045)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a6 (59046)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a6) [Reassembled in #27
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a6 (59046)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a7 (59047)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a7) [Reassembled in #29
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a7 (59047)	63	Access-Request id=218, Duplicate Request

image_en_ligne_2.png

4. Les captures br_outside montrent l'absence de paquets de 226 octets et l'écart dans les numéros de séquence ESP entre les paquets de 562 octets et les paquets de 1506 octets :

Source	Destination	Protocol	Sport	Dport	Length	IP ID	IP TTL	ESP Sequence	Wrong Sequence Number	Info
192.168.20.254	.99	ESP	4500	4500	1506	0x2d7e (11646)	64	6448		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x0b2c (2860)	64	6450	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x6ca9 (27817)	64	6451		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x51cf (20943)	64	6453	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x7d60 (32096)	64	6454		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x42de (17118)	64	6456	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x4553 (17747)	64	6457		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x7389 (29577)	64	6459	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x50f9 (20729)	64	6460		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x169f (5791)	64	6462	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	178	0x32d8 (13016)	64	6463		ESP (SPI=0x1592a843)

image_en_ligne_3.png

Points clés

- 226 octets sont manquants dans la capture br_outside, car ils sont abandonnés dans le pare-feu BR ASP avec la raison inattendue de suppression ASP de paquet.
- La suppression de paquets explique l’écart dans les numéros de séquence ESP.
- De plus, le numéro de séquence manquant dans la plage signifie que le paquet ESP de 226 octets a été généré par le pare-feu BR mais n'a pas été transmis par l'interface externe.
- Comme le paquet de 226 octets n’a pas été envoyé par l’interface externe du pare-feu BR, le pare-feu HQ ne l’a jamais reçu.
- L'absence du paquet de 226 octets dans le pare-feu HQ a entraîné l'échec du réassemblage de fragments, comme indiqué dans la section « Pare-feu HQ ».

Explication

Les résultats de la section d'analyse technique correspondent aux symptômes de l'ID de bogue Cisco CSCwp10123.

Vue d’ensemble à levier élevé des actions du pare-feu pour générer des paquets ESP et les transmettre par l’interface de sortie :

1. Le pare-feu reçoit des paquets fragmentés censés être envoyés via le tunnel VTI.
2. Si la longueur du paquet interne est supérieure à la taille MTU de l'interface moins la surcharge IPSEC, le paquet est fragmenté.
3. En fonction de la recherche dans la table de routage, le saut suivant est trouvé. Dans le cas de l'interface VTI, le saut suivant est l'adresse IP de l'homologue VTI.
4. En fonction de l’adresse de destination du tunnel, l’interface de sortie et le tronçon suivant sont identifiés (par exemple, l’interface externe).
5. Les paquets d’origine sont encapsulés dans des paquets ESP.
6. La recherche de contiguïté pour le saut suivant de l'étape 3 est effectuée et les paquets sont envoyés à l'interface de sortie.

En raison de l'ID de bogue Cisco CSCwp10123, pour les fragments (non initiaux) encapsulés ESP suivants, des paquets à l'étape 4 sont effectués une nouvelle recherche de route. Si le pare-feu dispose de routes plus spécifiques vers l'adresse IP (ou le sous-réseau) de l'homologue, les nouvelles routes sont utilisées à la place de la route du paquet initial. Dans cet exemple, l'adresse IP de l'interface du pare-feu HQ est x.x.x.99. Le pare-feu HQ annonce son sous-réseau externe au pare-feu BR via le protocole BGP (Border Gateway Protocol) exécuté sur le VTI :

<#root>

>

show route bgp

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRFGateway of last resort is 192.168.20.1 to network 0.0.0.0
```

B   x.x.x.96 255.255.255.224 [20/0] via 10.255.0.1, 13:57:43

<--BR firewall learns /27 route via BGP over VTI

<#root>

>

show bgp summary

BGP router identifier 192.168.179.10, local AS number 65001
BGP table version is 25, main routing table version 25
23 network entries using 4600 bytes of memory
24 path entries using 1920 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6960 total bytes of memory
BGP activity 23/0 prefixes, 24/0 paths, scan interval 60 secs
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

10.255.0.1 4 65000 762 761 25 0 0 13:59:01 18

>

show ip

…
Tunnel1 vti-hq 10.255.0.2 255.255.255.252 CONFIG <--

10.255.0.1

is the peer VTI IP
…

<#root>

>

show ip

…
Tunnel1 vti-hq 10.255.0.2 255.255.255.252 CONFIG <--

10.255.0.1

is the peer VTI IP in the same subnet
…

Le paquet ESP de 1 514 octets est envoyé à l’interface externe. Mais pour les 226 octets, le pare-feu à l'étape 3 effectue une recherche de route et trouve une route spécifique vers l'adresse IP homologue via le VTI. En d'autres termes, au lieu d'envoyer les paquets à l'interface de terminaison VPN, le pare-feu utilise l'interface VTI et tente de résoudre la contiguïté sur l'interface VTI. Puisque les interfaces VTI n'ont pas de concept de contiguïté, les paquets sont finalement abandonnés avec la raison d'abandon de paquet inattendu.

Pour contourner ce problème, sur CSF1230, l'utilisateur a inclus la liste de contrôle d'accès (ACL) dans la route-map. Après le déploiement de la stratégie, la liste de contrôle d'accès a refusé le sous-réseau externe HQ, supprimant ainsi la propagation du sous-réseau externe HQ du routage BGP. En raison de ce changement, les pare-feu BR ne reçoivent pas le préfixe de sous-réseau externe HQ sur l'interface du tunnel.

Q : Pourquoi les paquets de 266 octets sont-ils abandonnés après la migration de l'ASA vers le pare-feu sécurisé ?

A : La configuration du pare-feu ASA a explicitement bloqué la propagation du sous-réseau de l'interface externe de HQ vers les filiales.

ASA5508

```
router bgp 65000
...
  redistribute connected route-map BGP_RM
route-map BGP_RM permit 10
 match ip address bgp-connected-routes
access-list bgp-connected-routes standard deny x.x.x.96 255.255.255.224 <-- deny = do not redistribute
```

CSF1230

```
router bgp 65000
...
  redistribute connected route-map BGP_RM
route-map BGP_RM permit 40 <-- No match, means redistribute all connected routes
```

Motif

Le problème a été déclenché par une différence de configuration dans la redistribution de route

BGP entre l'ASA 5508 d'origine et le nouveau FTD 1230. L'ASA 5508 avait une liste de contrôle d'accès qui refusait la redistribution du sous-réseau x.x.x.96/27, tandis que le FTD 1230 était configuré pour redistribuer toutes les routes connectées. Cette différence de configuration a déclenché l'ID de bogue Cisco CSCwp10123.

Autres informations utiles

- ID de bogue Cisco CSCwp10123

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.